PERSPECTIVA DE MERCADO

WAF do cliente: A próxima fronteira de segurança

Christopher Rodriguez

SNAPSHOT EXECUTIVO

FIGURA 1

Snapshot executivo: Ameaças do cliente e soluções emergentes

Em 2018, os pesquisadores de segurança identificaram uma nova forma de crime virtual chamada de skimming de cartão on-line ou de skimming da Web. Os ataques Magecart exploraram uma tendência crescente de mudar a funcionalidade do aplicativo do servidor para o cliente. Os agentes de ameaças conseguiram injetar códigos mal-intencionados em fontes de aplicativos confiáveis, que foram executadas nos navegadores dos usuários longe da proteção de um WAF. Em última análise, os ataques representaram uma violação de dados que já vem sendo praticada há muito tempo, que expôs um link fraco nas práticas de segurança de aplicações Web empresariais.

Principais tópicos

- Os scripts do cliente são uma ferramenta valiosa na arquitetura de aplicativos, oferecendo os benefícios da experiência do usuário aprimorada, do desempenho do aplicativo, da análise e da segurança.
- Os scripts são onipresentes. Os sites da Web têm hoje dúzias de scripts diferentes, com os scripts do terceiros representando dois a cada três scripts.
- Os scripts do cliente representam um ecossistema de funcionalidade delicado, mas dinâmico, com muitas partes interessadas.
- Existem práticas recomendadas de linha de base para a segurança do cliente. No entanto, as complexidades e os desafios da segurança do cliente impulsionarão a demanda por soluções de segurança empresarial para esse vetor de ameaça.

Ações recomendadas

- As soluções disponíveis no mercado variam drasticamente de acordo com a funcionalidade. Para os compradores, o principal desejo é equilibrar a segurança com o requisito comercial de "não quebrar as coisas".
- A visibilidade e o controle do cliente não são uma área fácil ou familiar para muitos fornecedores. Os novos operadores de mercado considerarão cuidadosamente se devem criar suas próprias soluções ou escolher os recursos existentes para fazer parceria ou adquirir.
- Muitas organizações de TI não têm percepções sobre scripts ou ambientes do cliente. Poucas entendem os problemas de segurança. É necessário um alto grau de conhecimento do mercado, incluindo demonstrações, pesquisas, provas de conceitos e versões de avaliação.

Fonte: IDC, 2021

April 2021, IDC #US47623221

NOVOS DESENVOLVIMENTOS E DINÂMICAS DE MERCADO

Essa perspectiva de mercado da IDC fornece uma análise do vetor de ameaça, soluções emergentes e o futuro do mercado de Web Application Firewall (WAF) no lado do cliente.

A Akamai, a Cymatic, a PerimeterX e a Tala Security estão escalando novas trilhas, estendendo a proteção do WAF para lidar com ameaças do cliente. Os scripts do cliente representam um vetor de ameaça emergente, e o mercado de segurança está evoluindo para atender à necessidade.

Essas soluções de segurança são chamadas de "*WAF do cliente", anti-scripting ou segurança de script* , mas a terminologia pode ser confusa. Considere as seguintes opções:

- O WAF evoca um conjunto específico de controles que se aplicam a aplicações Web, embora os scripts do cliente sejam inerentemente um ponto de controle diferente no paradigma de segurança de aplicações.
- WAF do cliente é um termo útil para estabelecer uma conexão com um controle de segurança bem estabelecido no WAF, enquanto "segurança de script" pode ser um termo nebuloso e confuso por comparação.
- O termo "anti-scripting" generaliza scripts como uma tecnologia indesejada, com falhas ou totalmente mal-intencionada. Na realidade, os scripts representam uma ferramenta valiosa e poderosa na arquitetura de aplicativos.

Em geral, a IDC refere-se a essas soluções como WAF do cliente principalmente para os benefícios da familiaridade associada ao WAF. Além disso, o termo WAF do cliente mantém a possibilidade de expansão futura de tipos de ameaças do cliente além dos scripts.

Introdução

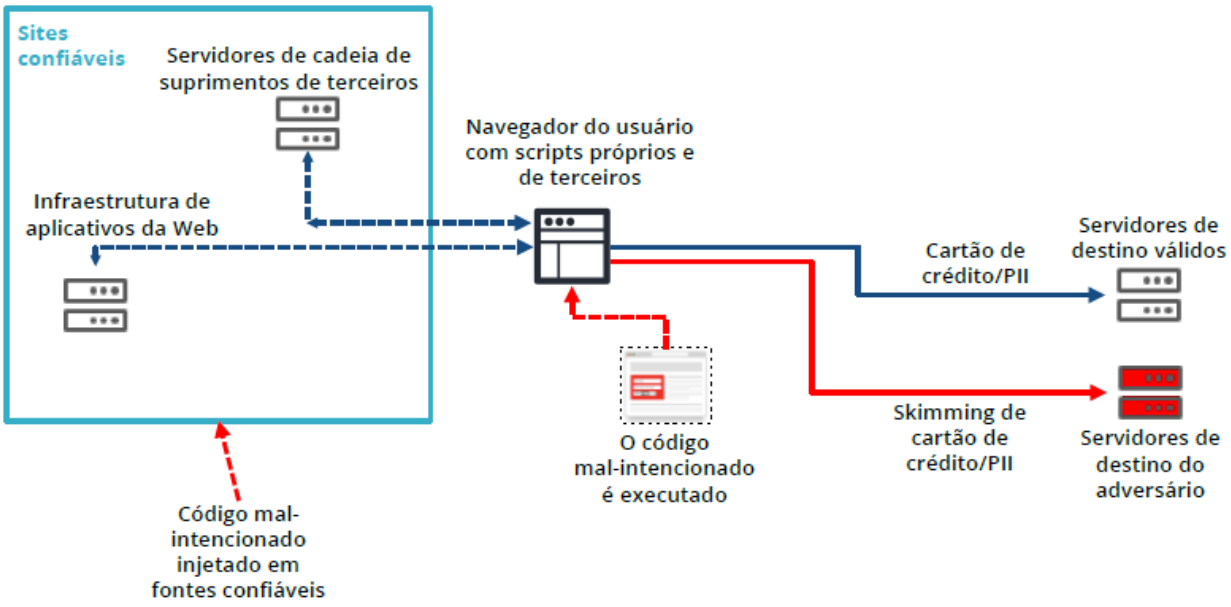
Uma nova técnica para roubo de dados de cartões de pagamento surgiu em 2018 e foi atribuída ao grupo de hackers Magecart. Os ataques do Magecart exploraram um novo vetor de ameaça, scripts que são executados em navegadores cliente. Uma vez detectada a campanha de ataque, investigações mostraram que o grupo Magecart havia comprometido por meses os sites de grandes empresas on-line, como Ticketmaster, NewEgg e British Airways.

A campanha do Magecart usou ataques do cliente para executar skimming na Web (que também pode ser chamado de skimming de cartão on-line ou form jacking). O skimming da Web é um aspecto altamente visível desse vetor de ameaça, mas o vetor de ameaça permite outros ataques, como ataques do tipo "watering hole" e criptojacking. O objetivo desses ataques pode variar, mas, em geral, a segurança do cliente tem potencial para campanhas de roubo de dados que resultam em violações de dados massivas e de longo prazo.

A Figura 2 fornece uma visão geral do ciclo de vida de um ataque no lado do cliente. Observe que o código malicioso é executado no navegador, longe das proteções oferecidas por um WAF. Além disso, códigos mal-intencionados podem ser injetados em fontes próprias e de terceiros.

FIGURA 2

Anatomia de um ataque de skimming da Web (no navegador)



Fonte: Akamai, 2021

Dinâmica do setor

O WAF do cliente é um mercado emergente com forte potencial de crescimento. Essa tecnologia aborda um vetor de ameaça emergente que é o resultado de uma mudança nas práticas de desenvolvimento de aplicações. A funcionalidade das aplicações vem mudando de servidores para clientes nos últimos anos e é improvável que a tendência diminua. A mudança na funcionalidade do servidor para o cliente descarrega as demandas de desempenho do servidor, permitindo assim um melhor desempenho e uma experiência mais interativa para os usuários finais. Como resultado, os scripts são ferramentas cada vez mais populares para alimentar experiências on-line interativas. Os scripts são usados para uma ampla e variada gama de finalidades legítimas, incluindo rastreamento, análise, experiência do usuário e segurança. Os scripts são onipresentes nos sites hoje, pois contêm 15 ou mais scripts diferentes, de acordo com algumas estimativas.

Além disso, a simplicidade do JavaScript tem impulsionado a adoção de scripts por profissionais que não são de TI. Os scripts permitem que unidades de negócios fora do departamento de TI criem e insiram código em ativos da Web para vários fins. Os scripts também facilitam a integração e a inserção de serviços de terceiros. No entanto, o aspecto de segurança dos scripts permanece amplamente ignorado, especialmente entre as organizações que continuam a se concentrar em ferramentas essenciais, como o WAF.

No geral, a ameaça não é bem compreendida. As violações mais amplamente discutidas nesta categoria se concentram em scripts de terceiros. A campanha do grupo Magecart fornece um exemplo pertinente. Nesse caso, os hackers do Magecart tinham acesso ao código de um parceiro fornecedor da organização visada e podiam inserir código mal-intencionado em scripts confiáveis. Para algumas organizações, o vetor de ameaça pode parecer uma prática em "mover as traves". Já é uma tarefa não trivial proteger um site contra as diversas ameaças enfrentadas por grandes empresas on-line, e a exigência de levar em conta as vulnerabilidades nos sistemas de parceiros parece praticamente injusta. Scripts de terceiros são os mais problemáticos, pois as organizações de TI não têm visibilidade ou controle sobre o código, as atualizações ou as alterações dos parceiros.

Infelizmente, o skimming da Web é apenas parte do problema, como scripts de terceiros representam apenas uma demografia dos scripts presentes na maioria das páginas da Web. Para referência, os pesquisadores da Akamai estimaram que cerca de 67% dos scripts vêm de terceiros. Por fim, a maioria das páginas da Web é um ecossistema de scripts de partes interessadas internas e terceiros. Esses sistemas internos também podem servir código mal-intencionado se os servidores forem sequestrados.

Há algumas práticas recomendadas que podem ajudar a reduzir o risco. Um controle mais rígido sobre scripts de terceiros é um início inteligente. As revisões regulares de código e os testes de aplicativos também são práticas confiáveis. Além disso, as organizações de TI podem aproveitar tecnologias como a Integridade de sub-recursos (SRI) para aplicar hash e detectar alterações nos scripts. Embora essas opções possam fornecer uma linha de base de proteção necessária, a história mostrou que agentes de ameaças sofisticados empregam consistentemente táticas avançadas e inteligentes para evitar a detecção. Como resultado, a SRI e outras práticas são pontos de partida úteis, mas serão limitadas contra ataques avançados.

Além disso, é improvável que os agentes de ameaça interrompam seus esforços, a menos que sejam forçados a fazê-lo. Desde os ataques do grupo Magecart, que ganharam as manchetes, os hackers modificaram esses ataques de várias maneiras. Por exemplo, os hackers podem visar as redes de anunciantes como um meio de injetar código malicioso por meio de anúncios em banners. Outros meios incluem o ataque a repositórios de código, como o GitHub. Esses repositórios incluem bibliotecas de código-fonte aberto e trechos de código que geralmente são reutilizados e confiáveis por muitas organizações para uso em suas aplicações da Web. Como resultado, essas fontes confiáveis representam um veículo potencial para a injeção de scripts maliciosos em sites que, de outra forma, seriam seguros.

Cada fornecedor aborda o problema de forma um pouco diferente. As soluções na tendência de mercado são amplamente implantadas por meio de tags JavaScript, o que permite que a função de segurança seja inserida antes que os scripts possam ser executados. A partir daí, as soluções divergem drasticamente. Os recursos principais tendem a incluir a visibilidade e o mapeamento de scripts e comunicações (por exemplo, origem e destino). Recursos adicionais incluem gerenciamento de vulnerabilidades, aplicação de políticas e detecção de atividades mal-intencionadas e eventos suspeitos. Recursos mais avançados são possíveis, como criptografia de chaves e dados incorporados, ofuscação de código, sandboxing e outras medidas defensivas. Por enquanto, a abordagem parece ser fornecer visibilidade e automação suficientes dos principais recursos de segurança. Embora medidas de detecção mais sofisticadas possam ser bem-vindas ao longo do tempo, a ênfase continua a ser o fornecimento de segurança suficiente sem interromper a experiência do usuário final ou, de outra forma, "quebrar" a funcionalidade do site.

Exemplos de fornecedores

Atualmente, existem algumas ofertas comerciais para o WAF do cliente, que variam em escopo e capacidade. Há alguns especialistas de mercado, incluindo a Digital.ai (anteriormente chamada de Arxan), a Source Defense, a Cymatic, Tala Security e a ChameleonX (adquirida pela Akamai em 2019). Outras têm portfólios amplos de segurança de aplicativos da Web. Por exemplo, a Akamai introduziu o Page Integrity Manager em 2020 como parte de sua abordagem para proteger contra ataques multivetoriais por meio de uma aplicação Web holística e de um portfólio de segurança de API. Da mesma forma, a PerimeterX introduziu sua oferta em 2019 como um complemento para sua solução de gerenciamento de bots empresariais. A mais nova participante é a CloudFlare, que apresentou sua nova solução em março de 2021. A IDC observa que essas empresas têm um histórico no gerenciamento de bots que pode ter ajudado a fornecer um nível de familiaridade com os sinais de segurança do cliente. O gerenciamento de bots é um processo desafiador de se fazer bem, e as melhores soluções tendem a empregar várias técnicas (incluindo JavaScript) para detectar e categorizar o comportamento dos bots.

Ataques ao cliente podem ser difíceis de detectar. No entanto, uma vez detectadas, essas ameaças são bastante claras em termos de custos financeiros para as empresas afetadas e seus clientes. Por exemplo, esses tipos de violações de dados podem ser medidos em termos do número de registros roubados de clientes. Os concorrentes existentes no espaço demonstraram um alto grau de eficácia na detecção e atenuação de ameaças baseadas em script. Isso faz com que os agentes de ameaça concentrem seus esforços em outro lugar, resultando em um jogo de ataque aleatório no setor. Para os invasores, o objetivo é encontrar sites desprotegidos ou pouco protegidos para atacar. Apesar da visibilidade dos ataques do Magecart, a conscientização do mercado sobre o vetor de ameaças permanece baixa, o que permite que os agentes de ameaças encontrem novos alvos. Todos esses fatores provavelmente aumentarão a conscientização geral do vetor de ameaça, o que impulsionará a demanda e atrairá empresas adicionais no mercado nos próximos anos.

Estratégias de mercado

As ameaças ao cliente serão um desafio para grandes empresas on-line enquanto os criminosos virtuais considerarem o vetor de ataque lucrativo. No entanto, esse é um tipo de ataque mais visado do que ataques transmitidos em massa, como ransomware. A maioria das organizações visadas levará tempo para detectar e atenuar ataques baseados em script. A conscientização geral do mercado sobre esses problemas também pode levar tempo e esforço para se elevar. Os fornecedores são desafiados a aumentar a conscientização por meio de treinamento contínuo, demonstrações e testes de prova de conceito.

Mais empresas provavelmente introduzirão seus próprios produtos e recursos. A Akamai introduziu o Page Integrity Manager há um ano para tratar da superfície de ataque em expansão criada por scripts carregados em navegadores, onde as informações de identificação pessoal (PII) são enviadas e acessadas. Também é aqui que as ameaças do cliente proliferaram em 2020, como o uso da Internet para transações se acelerou no ambiente da COVID-19.

A CloudFlare é a mais recente adição ao mercado, apresentando uma nova solução chamada CloudFlare Page Shield. Antes deste acordo, a CloudFlare abordou esse vetor de ameaça por meio de uma parceria tecnológica com a Tala Security.

Embora a CloudFlare tenha decidido desenvolver seus próprios recursos de segurança no lado do cliente, a IDC observa que a abordagem pode não ser tão fácil para outras pessoas seguirem. Para a maioria dos fornecedores no mercado, o desenvolvimento de recursos WAF do cliente foi precedido por técnicas de detecção de bots que aproveitam clientes JavaScript. As soluções WAF legadas não têm esses recursos ou outra experiência com código do cliente.

Para fornecedores que estão reforçando suas linhas de produtos de segurança de aplicativos Web e API, a aquisição de soluções especializadas pode apresentar a melhor opção até mesmo para o campo de atuação. A aquisição da ChameleonX pela Akamai fornece um exemplo dos benefícios potenciais da combinação de tecnologias de uso específico com escala de nuvem. O Page Integrity Manager agora protege mais de 3,7 bilhões de visualizações de página por mês, analisando 6,4 bilhões de execuções de script todos os dias. Aproximadamente 40 milhões de interações suspeitas e mal-intencionadas com o usuário final são observadas semanalmente, o que permite que a Akamai forneça notificações em tempo real, análise de causa raiz, atenuação imediata e criação de políticas de automação.

PONTO DE VISTA DA IDC

Os ataques no lado do cliente serão uma crescente lacuna de segurança enquanto os criminosos virtuais perceberem que o vetor de ataque é lucrativo, o que pode durar muitos anos. Um motivo significativo para isso é o fato de que o vetor de ameaça ao cliente não é bem compreendido. Tradicionalmente, as soluções WAF funcionam analisando o tráfego de aplicações Web direcionado ao servidor Web. Como o JavaScript se tornou mais popular ao longo dos anos, quantidades significativas de funcionalidades migraram para o navegador do cliente. Mas muitas organizações ignoram esses fatos ou não fizeram uma avaliação adequada dos riscos e das implicações de segurança dessa migração da funcionalidade da Web para o navegador do cliente.

O fato de esse tipo de ataque ser mais visado do que ataques transmitidos em grande escala, como ransomware, está contribuindo ainda mais para altos níveis de confusão no mercado. Por exemplo, a maioria das organizações está bem familiarizada com os tipos de ataques tratados pelo WAF e pelas soluções de atenuação de DDoS. O risco de segurança apresentado por bots indesejados ou mal-intencionados é outra prática que está ganhando conhecimento geral. No entanto, áreas mais recentes, como segurança de API e segurança do cliente, representam áreas de risco emergentes que simplesmente não são visíveis e, portanto, representam um risco significativo, muito parecido com a metade submersa de um iceberg (veja a Figura 3).

FIGURA 3

O aplicativo da Web e o iceberg da segurança de API

Fonte: IDC, 2021

Depois que uma organização entende o vetor de ameaça potencial, o processo de catalogar e conhecer os scripts executados em um ambiente de TI complexo com vários domínios, páginas da Web e aplicativos da Web pode representar uma tarefa hercúlea. No momento dos ataques do Magecart, o processo de detecção de scripts maliciosos injetados representou uma revisão manual, linha por linha, do código para detectar alterações. O processo é mais simplificado agora, pois os pesquisadores entendem os problemas subjacentes e as melhores práticas. No entanto, o ponto é que a maioria das organizações visadas levará tempo para detectar e atenuar ataques baseados em script, pois leva tempo para entender o vetor de ameaça e tempo adicional para identificar falhas ou explorações de segurança existentes. Além disso, o vetor de ameaça é um alvo em movimento, pois 75% dos scripts são alterados a cada trimestre. Cada nova alteração abre a possibilidade de introduzir novas vulnerabilidades e códigos mal-intencionados.

No entanto, o tempo é essencial. Já as violações conhecidas devido a ataques do cliente duraram muito tempo e forneceram aos invasores meses de vantagem. Naquela época, um número incontável de cartões de crédito, bem como outras informações pessoais, foram roubados. Quando um ataque é detectado, os invasores ficam livres para fechar a loja e começar de novo com a próxima vítima. Essencialmente, os ataques do cliente levam um tempo enorme para serem detectados, e esse desequilíbrio é uma enorme vantagem para os criminosos virtuais e deve ser reduzido.

Portanto, o tempo é o maior obstáculo para o setor de segurança instruir e melhorar a conscientização do comprador sobre o problema. Os fornecedores são desafiados a aumentar a conscientização por meio de treinamento contínuo, demonstrações e testes de prova de conceito. A Akamai, por exemplo, está oferecendo uma versão do Page Integrity Manager para avaliação gratuita. A solução fornece uma visão geral do ecossistema de scripts de páginas da Web direcionadas, juntamente com a análise dos vários scripts, vulnerabilidades e fatores de risco. Outros fornecedores também oferecem versões de avaliação, demonstrações e recursos informativos.

A IDC louva essas abordagens. Nada transmite melhor a urgência de uma situação ou o valor e a eficácia de uma solução de segurança do que uma prova de conceito. Para os fornecedores, o benefício de uma possível conversão de assinatura premium é claro. Os compradores também se beneficiam substancialmente, ganhando visibilidade em um vetor de ameaça que tradicionalmente tem sido um ponto cego completo para a maioria das organizações.

Além do horizonte, a IDC monitorará o mercado de WAF do cliente para entender seu impacto em mercados estabelecidos, como WAF, atenuação de DDoS, gerenciamento de bots e prevenção contra fraudes on-line. Assim que o ponto cego de segurança do cliente for tratado, serão necessárias discussões mais aprofundadas sobre o impacto dos recursos de visibilidade e aplicação em potencial do cliente, como um ponto de controle de segurança.

SAIBA MAIS

Pesquisa relacionada

- *IDC FutureScape: Worldwide Future of Trust 2021 Predictions* (IDC #US46912920, outubro de 2020)
- *Pervasive Application Edge Defense: An Application-Based Framework for Trust* (IDC #US46810219, setembro de 2020)
- *IDC Market Glance: Software-Defined Secure Access, 2Q20* (IDC #US46291520, maio de 2020)
- *Worldwide Internet Defense Forecast, 2020-2023: Infrastructure and Application Security Drive Business Value* (IDC #US46022619, fevereiro de 2020)
- *Security Convergence at the Edge: Emerging Pervasive Data Defense and Response Platforms* (IDC #US46075520, fevereiro de 2020)

Sinopse

Essa perspectiva de mercado da IDC fornece uma análise do vetor de ameaça, soluções emergentes e o futuro do mercado de WAF do cliente. Poucas organizações de TI têm um entendimento completo das ameaças direcionadas a scripts do cliente que são executados em seus ambientes da Web. Os criminosos virtuais têm visado scripts do cliente como um meio de executar códigos mal-intencionados de forma sorrateira para obter um enorme ganho financeiro, sem o risco de serem pegos. À medida que esse vetor de ameaça se tornar mais pronunciado nos próximos anos, a demanda por soluções WAF do cliente empresarial deverá crescer continuamente.

"O script do cliente é a próxima fronteira de segurança. Os criminosos virtuais continuam incansáveis em sua busca por explorações lucrativas e encontraram uma nova lacuna nas pilhas de segurança digital empresarial", afirma Christopher Rodriguez, gerente de pesquisa da IDC Network Security Products and Strategies.

Sobre a IDC

A International Data Corporation (IDC) é a principal fornecedora global de inteligência de mercado, serviços de consultoria e eventos para os mercados de tecnologia da informação, telecomunicações e tecnologia do consumidor. A IDC ajuda profissionais de TI, executivos de negócios e a comunidade de investimentos a tomar decisões baseadas em fatos sobre compras de tecnologia e estratégia de negócios. Mais de 1.100 analistas da IDC oferecem experiência global, regional e local em oportunidades e tendências de tecnologia e do setor em mais de 110 países em todo o mundo. Há 50 anos, a IDC vem fornecendo percepções estratégicas para ajudar nossos clientes a atingirem seus principais objetivos de negócios. A IDC é uma subsidiária da IDG, a empresa líder mundial em mídia tecnológica, pesquisa e eventos.

Sede global

5 Speen Street
Framingham, MA 01701
EUA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com